Порядок работы NAT

Содержание

Введение

В этом документе показывается, что порядок обработки транзакций с использованием Network Address Translation (NAT) основан на данных о том, проходит ли пакет из внутренней сети во внешнюю, или наоборот.

Предварительные условия

Требования

Использование данного документа требует наличия следующих знаний:

- Network Address Translation (NAT). Подробнее о NAT см. "Работа NAT".

Используемые компоненты

Данный документ не ограничен отдельными версиями программного и аппаратного обеспечения.

Примечание: Сведения, содержащиеся в данном документе, основаны на программном обеспечении Cisco IOS, релиз 12.2(27)

Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

Обзор NAT

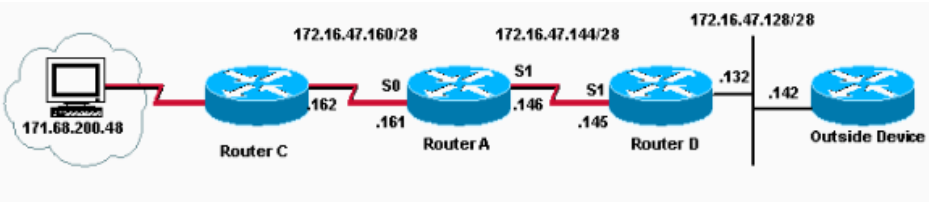
В следующей таблице показано, что когда NAT работает из глобальной в локальную сеть и наоборот, трансляция для каждого потока отличается.

Внутренний-внешнему	Внешний-внутреннему

• Если IPSec, то проверить входной список доступа • дешифрование - для CET (Cisco Encryption Technology) или IPSec • проверить список доступа ввода • проверить ограничения входной скорости • учет входных данных • политика маршрутизации • маршрутизация • перенаправить к веб-кэшу • **NAT изнутри наружу (трансляция локальных адресов в глобальные)** • крипто (проверка схемы и метки на наличие шифрования) • проверить выходной список доступа • проверка (Context-based Access Control (CBAC)) • перехват TCP • шифрование • Формирование очереди	• Если IPSec, то проверить входной список доступа • дешифрование - для CET или IPSec • проверить входной список доступа • проверить ограничения входной скорости • учет входных данных • **NAT снаружи внутрь (трансляция глобальных адресов в локальные)** • политика маршрутизации • маршрутизация • перенаправить к веб-кэшу • крипто (проверка схемы и метки на наличие шифрования) • проверить выходной список доступа • проверка CBAC • перехват TCP • шифрование • Формирование очереди

Конфигурация и выходные данные NAT

Следующий пример демонстрирует, как порядок действия может повлиять на NAT. В данном случае показаны только NAT и маршрутизация.



В приведенном выше примере маршрутизатор A настроен на преобразование внутреннего локального адреса 171.68.200.48 в адрес 172.16.47.150, как показано ниже.

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
```

```
ip nat inside source static 171.68.200.48 172.16.47.150

!--- Эта команда создает статическую трансляцию NAT
!--- между адресами 171.68.200.48 и 172.16.47.150

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Ethernet0
no ip address
shutdown
!
interface Serial0
ip address 172.16.47.161 255.255.255.240
 ip nat inside

!--- Настраивает Serial0 как внутренний интерфейс NAT

no ip mroute-cache
no ip route-cache
no fair-queue
!
interface Serial1
ip address 172.16.47.146 255.255.255.240
 ip nat outside

!--- Настраивает Serial1 как внешний интерфейс NAT

no ip mroute-cache
no ip route-cache
!
no ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145

!--- Настраивает маршрут по умолчанию к 172.16.47.145


ip route 171.68.200.0 255.255.255.0 172.16.47.162
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password ww
login
!
end
```

Таблица преобразований показывает, что предполагаемое преобразование существует.

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---
```

Следующие выходные данные взяты из маршрутизатора A со включенными командами **debug ip packet detail** и **debug ip nat** и эхо-тестом из устройства 171.68.200.48, направленным в 172.16.47.142.

Примечание: команды отладки генерируют значительный объем выходных данных. Используйте их только тогда, когда трафик в IP-сети низкий, чтобы не снизить быстродействие других процессов системы. Перед началом работы с командами **debug** ознакомьтесь с разделом "Важные сведения о командах отладки".

```
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
   ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
   ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
   ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
   ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
   ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
```

```
   ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
   ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
   ICMP type=3, code=1
```

Поскольку в приведенных выше выходных данных нет сообщений отладки NAT, получается, что существующее статическое преобразование не используется и у маршрутизатора в его таблице маршрутизации нет маршрута для адреса назначения (172.16.47.142). Результатом немаршрутизируемого пакета является сообщение ICMP о недостижимости, которое отправляется на внутреннее устройство.

Однако для маршрутизатора A имеется маршрут 172.16.47.145 по умолчанию. Почему маршрут не признается маршрутизируемым?

В маршрутизаторе A настроена команда **no ip classless**, что означает, что если пакет направлен для адреса "крупной" сети (в данном случае 172.16.0.0), для которой в таблице маршрутизации существуют подсети, то маршрутизатор не полагается на маршрут по умолчанию. Другими словами, задание команды **no ip classless** отключает возможность маршрутизатора искать маршрут с самым длинным совпадением битов. Чтобы изменить это поведение, необходимо настроить **ip classless** на маршрутизаторе A. Команда **ip classless** по умолчанию включена на маршрутизаторах Cisco с версиями IOS 11.3 и более поздними.

```
Router-A#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Router-A(config)#ip classless
Router-A(config)#end

Router-A#show ip nat translation
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---
```

Повторяя предыдущий это-тест, можно увидеть, что пакет транслируется, и эхо-тест является удачным.

```
Ping Response on device 171.68.200.48

D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:

Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.47.142:
   Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum =  10ms, Average =  2ms

Debug messages on Router A indicating that the packets generated by device
171.68.200.48 are getting translated by NAT.

Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=171.68.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0

Router-A#undebug all
All possible debugging has been turned off
```

Приведенный выше пример показывает, что в случае перехода пакета изнутри наружу маршрутизатор NAT проверяет таблицу маршрутизации на наличие маршрута к внешнему адресу перед тем как продолжить преобразование пакета. Поэтому важно, чтобы маршрутизатор NAT имел допустимый маршрут для внешней сети. Маршрут к сети назначения должен быть известен через интерфейс, определенный в конфигурации маршрутизатора как NAT наружу.

Важно отметить, что возвращаемые пакеты транслируются до их маршрутизации. Поэтому маршрутизатор NAT должен также иметь в своей таблице маршрутизации действительный маршрут для внутреннего локального адреса.

Дополнительные сведения

- **Настройка трансляции сетевых адресов: Начало работы**
- **Проверка работоспособности, поиск и устранение основных неисправностей NAT**
- **NAT: Локальные и глобальные определения**
- **Как многоадресное преобразование NAT работает на маршрутизаторах Cisco?**
- **Страница поддержки NAT**
- **Техническая поддержка - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92039/5.shtml